Dimensional Dual Hyperovals admitting Large Automorphism Groups(Group Theory and Related Topics)

AUTHOR(S):

吉荒, 聡

CITATION:

吉荒, 聡. Dimensional Dual Hyperovals admitting Large Automorphism Groups(Group Theory and Related Topics). 数理解析研究所講究録 2007, 1564: 1-13

ISSUE DATE:

2007-07

URL:

http://hdl.handle.net/2433/81153

数理解析研究所講究録
第1564巻 2007年 1-13

Dimensional Dual Hyperovals admitting Large Automorphism Groups

吉荒 聡 (Satoshi Yoshiara)
東京女子大学・数理学科
Department of Mathematics, Tokyo Woman's Christian University
167-8585 東京都杉並区善福寺 2-6-1
yoshiara@lab.twcu.ac.jp

1 はじめに

この論説は、２００６年１２月１８日京都大学会館で行われた集会における筆者の講演の大要をまとめたものである。大きな自己同型群を持つ高次元の双対超卵形に対する、最近の３つの結果の紹介とその意味、証明の大筋の解説、が主な内容である。

定義 1 r を素数のべき、d を自然数とする。また U を $GF(r)$ 上のベクトル空間で、その次元 $\dim(U)$ が $2d+1$ 以上であるものとする。U の $d+1$ 次元の部分空間の集まり $\mathcal{S}$ が、次の条件 *(DHO1)-(DHO3)* を満たすとき、$\mathcal{S}$ は $GF(r)$ 上 d 次元の**双対超卵形** *(d-dimensional dual hyperoval over $GF(r)$)* と呼ばれる。以下、これを略して *d-DHO* と書く。

(DHO1) 任意の相異なる $X, Y \in \mathcal{S}$ に対して $\dim(X \cap Y) = 1$.

(DHO2) 任意の互いに異なる $X, Y, Z \in \mathcal{S}$ に対して $X \cap Y \cap Z = \{0\}$.

(DHO3) $|\mathcal{S}| = ((r^{d+1}-1)/(r-1)) + 1$.

条件 *(DHO1)* と *(DHO2)* を満たす部分空間は高々 $((r^{d+1}-1)/(r-1))+1$ 個しか存在しないことが示せるので、条件 *(DHO3)* は、条件 *(DHO1),(DHO2)* を満たすような最大の部分空間族を考えるという意味である。

$\mathcal{S}$ に属する部分空間全体が生成する U の部分空間を $\mathcal{S}$ の **ambient space** と呼び、時々 $\mathbf{A}(\mathcal{S})$ と表す。$GF(r)$ 上の有限次元ベクトル空間 V に対して、V を *ambient space* とする *d-DHO* $\mathcal{S}$ のことを、*"d-DHO over $GF(r)$ in V (または $PG(V)$)"* と表現することもある。

$$\mathbf{A}(\mathcal{S}) := \langle X \mid X \in \mathcal{S} \rangle. \tag{1}$$

d-DHO $\mathcal{S}$ の自己同型群とは、その *ambient space* $V = \mathbf{A}(\mathcal{S})$ が定める射影空間 $PG(V)$ の自己同型であって、$\mathcal{S}$ のメンバーを $\mathcal{S}$ のメンバーに移すようなもの全体が写像の合成に関してなす群のことである。この群を $\mathrm{Aut}(\mathcal{S})$ と記す。

$$\mathrm{Aut}(\mathcal{S}) := \{\sigma \in \mathrm{Aut}(PG(\mathbf{A}(\mathcal{S}))) \mid X^\sigma \in \mathcal{S} (\forall X \in \mathcal{S})\}. \tag{2}$$

射影空間 $PG(V)$ の自己同型群 $\mathrm{Aut}(PG(V))$ とは、V 上の半線形射影変換全体のなす群であった。そこで、$\dim(V)=n$ とすれば $Aut(PG(V))$ は射影線形群 $PGL(V)\cong PGL(n,r)$ と体 $GF(r)$ の自己同型 $\mathrm{Gal}(GF(r)/GF(p))\cong Z_e$ の半直積である。ここで $r=p^e$, p は素数とし、記号 Z_e は位数 e の巡回群を表す: $\mathrm{Aut}(PG(V))\cong PGL(n,r):Z_e$.

d-DHO という対象を研究する意味について一言述べておく。より詳しくは、以前の集会における私の講演録 [11] や私のサーベイ [12]、最近の論文 [4] の序文 1.1 を参照されたい。$d=1$ に対する d-DHO は、デザルグ射影平面上の dual hyperoval という古典的な対象であり、次の対象[1]を結ぶ接点になっている。

o-polynomial という置換多項式 (2 次式の一般化) の部分族、
translation planes という射影平面の部分族、
位数 (s,s) の generalized quadrangles の部分族。

この意味で、1-DHO は、階数の低い有限幾何の研究における中心的対象であり、豊かな数学を生み出している。これの類似を高次元 $(d\geq 2)$ で展開することによって、楽しみましょうというのが、私の意図である。

d-DHO $\mathcal{S}$ の自己同型群 $\mathrm{Aut}(\mathcal{S})$ は自然に $\mathcal{S}$ のメンバー上の置換を引き起こすが、この作用は忠実であることが分かる。この自然な作用を通じて $\mathrm{Aut}(\mathcal{S})$ を $((r^{d+1}-1)/(r-1))+1$ 次の対称群 $Sym(\mathcal{S})$ の部分群と見ることが出来る。この置換群 $\mathrm{Aut}(\mathcal{S})$ が $\mathcal{S}$ 上に高い可移性を持つような d-DHO $\mathcal{S}$ について調べてみようというのが、この講演の主題である。

2 知られている DHO の例

$GF(q)$ 上定義された d-DHO $\mathcal{S}$ と $\mathcal{T}$ がある。Ambient space $V=\mathbf{A}(\mathcal{S})$ から $W=\mathbf{A}(\mathcal{T})$ への $GF(q)$ 上の全射半線形変換で、$\mathcal{S}$ を $\mathcal{T}$ に移すものがあるとき、$\mathcal{T}$ は $\mathcal{S}$ の **quotient** である ($\mathcal{S}$ は $\mathcal{T}$ の **cover** である) という。d-DHO $\mathcal{S}$ を cover するような d-DHO が自分自身以外に存在しないとき、$\mathcal{S}$ は **simply connected** であるという。

現在知られている simply connected な DHO の例とその ambient space の次元、自己同型群、及びそのメンバー上の置換群としての可移性については、表 1 のようにまとめられる。Taniguchi の DHO は Veronesean DHO の変形 (deformation) とも言えるものであるが、その自己同型群の具体形については、この報告集中の谷口氏の記事を見られたい。これらの DHO は、任意の自然数 e に対する $q=2^e$ 元体上で定義される。一方、Buratti-Del Fra の DHO は、Huybrechts の DHO の変形と見なせるが、これらの DHO が定義されるのは二元体に限る。$\mathcal{S}^{d+1}_{\sigma,\phi}$ と記された DHO [8] も、二元体上のみで定義され、σ は $GF(2^{d+1})$ の絶対ガロア群 $\mathrm{Aut}(GF(2^{d+1}))$ の生成元、ϕ は $GF(2^{d+1})$ 上の全単射で、o-関数により引き起こされるものである。$\sigma=\phi$ の時には、$\mathcal{S}^{d+1}_{\sigma,\phi}$ は Huybrechts DHO により cover されるので simply connected ではないが、これ以外の場合には、殆ど simply connected である。

[1]正確な定義は、ここでは必要ないので、省略する。

Table 1: Known simply connected d-DHOs ($d \geq 2$)

Name	$\dim(\mathbf{A}(\mathcal{S}))$	q	$\mathrm{Aut}(\mathcal{S})$	Transitivity
Veronesean	$(d+1)(d+2)/2$	2^e	$PGL(d+1,q)$	intransitive
Taniguchi	$(d+1)(d+2)/2$	2^e		intransitiive
Huybrechts	$(d+1)(d+2)/2$	2	$2^{d+1} : SL_{d+1}(2)$	2-transitive
Buratti and Del Fra	$(d+1)(d+2)/2$	2	$2^{d+1} : (2^d : SL_d(2))$	transitive but not 2-transitive
$\mathcal{S}^{d+1}_{\sigma,\phi}(\phi \neq \sigma^{-1})$	$2(d+1)$	2	$2^{d+1} : (Z_{2^{d+1}-1} : Z_{d+1})$ $d \geq 3$	2-transitive if $\phi \in \mathrm{Aut}(GF(2^{d+1})$
$\mathcal{S}^{d+1}_{\sigma,\phi}(\phi \neq \sigma^{-1})$	$2(d+1)$	2	$Z_{2^{d+1}-1} : Z_{d+1}$	intransitive if $\phi \notin \mathrm{Aut}(GF(2^{d+1})$
$\mathcal{S}^{d+1}_{\sigma,\phi}(\phi = \sigma^{-1})$	$2d+1$	2	$2^{d+1} : (Z_{2^{d+1}-1} : Z_{d+1})$	2-transitive
Mathieu	6	4	$M_{22}.2$	$2-$intransitive

3 二重可移な DHO

3.1 Huybrechts-Pasini の結果

$GF(q)$ 上の d-DHO $\mathcal{S}$ に対して、自己同型群 $\mathrm{Aut}(\mathcal{S})$ が $\mathcal{S}$ のメンバー上に可移 (resp. 二重可移) なときに、$\mathcal{S}$ は**可移** (resp. **二重可移**) であるということにする。

表 1 を見る限り、二重可移な DHO の殆どが二元体上定義されたものである。実際、「$GF(q)$ 上定義された二重可移な d-DHO に関しては、$q > 2$ かつ $d \geq 2$ のときには、Mathieu DHO に限る」と信じられていた。その一つの根拠は次の Huybrechts と Pasini による定理 [6] である。

定理 2 *$\mathcal{S}$ を $GF(q)$ 上定義された二重可移な d-DHO とする。このとき、次のいずれかが成立する。*

(1) $q = 2$.

(2) $\mathcal{S}$ は *Mathieu DHO* である。従って $q = 4$, $d = 2$, $\mathrm{Aut}(\mathcal{S}) \cong M_{22}.2$.

(3) q は奇素数べき、d は偶数、$|\mathcal{S}|$ は 2 のべきで、$\mathrm{Aut}(\mathcal{S})$ は $Z_{q^{d+1}-1} : Z_{d+1}$ の部分群に同型。

この定理 2 には、次のような点で不満が残る。まず、$q = 2$ 元体上で定義された二重可移な DHO については何も結果が得られていない。次に、実際には起こりそうもない場合 (3) が残っている。更に、証明を見ると、そこでは「二重可移群の分類」という、有限単純群分類結果に依存した深い結果以外にも、「旗上可移な linear spaces の分類」という、

これまた有限単純群の分類に依存し、しかも多くの人々が関わって得られた結果が使われている。これは、論文 [6] では、d-DHO そのものの分類を試みたのではなく、d-DHO から生じるインシデンス幾何の分類を考えたことに起因する。

3.2 二重可移な DHO に対する、より精密な結果

そこで、上の結果 2 の精密化を、なるべく直接に証明しようと試みるのは自然であろう。今年の春に、私は次の結果を得た [13]。

定理 3 $\mathcal{S}$ を $GF(q)$ 上定義された d-*DHO* で、その自己同型群の部分群 G が $\mathcal{S}$ 上二重可移であるものとする。このとき、次のいずれかが成立する。

(1) $q=2$ であって、G はアフィン型の二重可移群である。すなわち、$\mathcal{S}$ 上正則に作用する G の正規部分群 N が存在して $G=N:G_X$ (G_X は $\mathcal{S}$ 一つのメンバー X の G における *stabilizer*) という形に分解する。しかも、*stabilizer* G_X の可能性は次のように制限される。

- *(1-a)* G_X は $Z_{2^{d+1}-1}:Z_{d+1}$ の部分群。
- *(1-b)* $d+1$ の約数 l $(2\le l\le d+1)$ が存在して、G_X は $PSL_l(2^{(d+1)/l})$ を正規部分群に持ち、$\mathrm{Aut}PSL_l(2^{(d+1)/l})$ の部分群と同型である。
- *(1-c)* d は奇数で、$(d+1)/2$ の約数 l $(2\le l\le (d+1)/2)$ が存在して、G_X は $(PSp_{2l}(2^{(d+1)/(2l)}))'$ を正規部分群に持ち、$\mathrm{Aut}(PSp_{2l}(2^{(d+1)/(2l)}))$ の部分群と同型である。
- *(1-d)* $d+1$ は 6 の倍数で、G_X は $(G_2(2^{(d+1)/6}))'$ を正規部分群とし、$\mathrm{Aut}(G_2(2^{(d+1)/6}))$ の部分群と同型である。
- *(1-e)* $d=3$ であって、G_X は A_6, S_6 または A_7 に同型である。

(2) $\mathcal{S}$ は *Mathieu DHO* である。このとき $q=4$, $d=2$, $G\cong M_{22}$ *or* $M_{22}.2$.

特に Huybrechts-Pasini の定理 2 における残された場合 (3) が消去されたので、「$q>2$, $d\ge 2$ に対する $GF(q)$ 上定義された二重可移な d-DHO は Mathieu DHO に限る」という、上記の予想が証明された。更に、二元体上定義された二重可移な d-DHO に対しても、この定理はかなり詳しい情報を提供する。定理 3 の場合 (1-c), (1-d), (1-e) は、どれも起こらないように思われる。特に (1-e) においては $d=3$ という大きな制限があるため、これを消すのは単なる力仕事であるように思うが、私の怠慢のため、実行していない。

定理 3 の証明においても、やはり二重可移群の分類は必要になる。従って、有限単純群の分類は欠かせない。一方、旗上可移な linear space の分類は不要になる。この部分は、後述するように、一つのメンバーの stabilizer の構造を（二重可移群の分類を使って）二通りに求めて、その結果を比較することで済むのである。更に、定理 2 の場合 (3) の消去にあたっては、extraspecial 2-group や (核が elementary abelian 2-group であるような) Frobenius 群の通常表現論が使用される。これから得られる ambient space の次元の下からの評価と、「$q>2$ ならば、$GF(q)$ 上定義された d-DHO の ambient space の次元は $(d+1)(d+2)/2$ 以下である」という結果 [10] から矛盾が導ける。

Table 2: Doubly transitive groups of semisimple type [2]

	N	$\|\Omega\|$		$\max \|G/N\|$
$(S1)$	A_n	n	$n \geq 5$	2
$(S2)$	$PSL_l(q)$	$(q^l-1)/(q-1)$	$l \geq 2$	$(l, q-1)e$ $(q = p^e)$
$(S3)$	$PSU_3(q^2)$	q^3+1	$q \neq 2$	$(3, q+1)2e$
$(S4)$	${}^2B_2(q)$	q^2+1	$q = 2^{2m+1}, m \geq 1$	$2m+1$
$(S5)$	${}^2G_2(q)$	q^3+1	$q = 3^{2m+1}, m \geq 1$	$2m+1$
$(S6)$	$Sp_{2l}(2)$	$2^{2l-1} \pm 2^{l-1}$	$l \geq 3$	1

	N	$\|\Omega\|$	$\max \|G/N\|$		N	$\|\Omega\|$	$\max \|G/N\|$
$(S7)$	$PSL_2(11)$	11	2	$(S12)$	M_{22}	22	2
$(S8)$	$PSL_2(8)$	28	3	$(S13)$	M_{23}	23	1
$(S9)$	A_7	15	1	$(S14)$	M_{24}	24	1
$(S10)$	M_{11}	11, 12	1	$(S15)$	HS	176	1
$(S11)$	M_{12}	12	1	$(S16)$	$Co3$	276	1

Table 3: Doubly transitive groups of affine type [7]

	$\leq G_X$	$G_X \leq$	$\|\Omega\|$
$(Af1)$		$\Gamma L_1(p^m)$	p^m
$(Af2)$	$SL_l(p^{m/l})$	$GL_l(p^{m/l})Z_{m/l}$	p^m $(l\|m, l \geq 2)$
$(Af3)$	$Sp_{2l}(p^{m/2l})'$	$Sp_{2l}(p^{m/2l})Z_{m/l}$	p^m $(l\|2m, l \geq 2)$
$(Af4)$	$G_2(p^{m/6})'$	$G_2(p^{m/6})Z_{m/6}$	p^m $p = 2, (6\|m)$
$(Af5)$		$N_{GL_m(p)}(R), R \cong 2_-^{1+2}$	$5^2, 7^2, 11^2, 23^2$
$(Af6)$		$N_{GL_4(3)}(R), R \cong 2_-^{1+4}$	3^4
$(Af7)$	$SL_2(5)$	$SL_2(5)$	$3^4, 11^2, 19^2, 29^2, 59^2$
$(Af8)$	A_n	$A_n, \quad n = 6, 7$	2^4
$(Af9)$	$SL_2(13)$	$SL_2(13)$	3^6

3.3 定理 3 の証明のあらまし

$\mathcal{S}$ を $GF(q)$ 上定義された d-DHO とし、V をその ambient space とする。$\bar{G}$ は $\mathrm{Aut}(\mathcal{S})$ の部分群で $\mathcal{S}$ 上二重可移に作用するものとする。$\mathrm{Aut}(\mathcal{S})$ は $\mathrm{Aut}(PG(V)) = \Gamma L(V)/Sc(V)$ の部分群として定義されていた。ここで $\Gamma L(V) \cong GL(V) : \mathrm{Aut}(GF(q))$ は V 上の $GF(q)$-半線形変換全体のなす群であり、$Sc(V) \cong GF(q)^\times$ は V 上のスカラー変換全体のなす、位数 $q-1$ の巡回群である。$\bar{G}$ 自身ではなく、$\Gamma L(V)$ におけるその逆像 G を考えるのが第一のポイントである。

$q = p^e$, p は素数、とする。$\mathcal{S}$ の一つのメンバー X の stabilizer G_X は、$Sc(V)$ を含み、ベクトル空間 X 上に忠実な $GF(p)$-線形変換を引き起こす。従って G_X は $GF(p)$ 上の $e(d+1)$ 次元ベクトル空間と見た X 上の全単射線形変換のなす群 $GL(X) \cong GL_{e(d+1)}(p)$ の部分群と同型であるが、二重可移性の仮定から、G_X は X の非零ベクトルの集合 $X^\#$ 上に可移に作用する。このとき、X に対応する translation group $\tilde{X}$ を考えれば、半直積 $\tilde{X} : G_X$ は X 上の（アフィン型）二重可移群であるから、二重可移群の分類により決定されている。結果は表 3 にまとめられている。この表の 4 列目の値 $|\Omega|$ は置換表現の次数を示し、一点 $X \in \Omega$ の stabilizer G_X の最小と最大の可能性が、2 列目と 3 列目に現れている。これから $G_X/Sc(V)$ の可能性が限定される。

一方、$G/Sc(V)$ は $\mathcal{S}$ 上の二重可移置換群であるから、その可能性は二重可移群の分類により限定できる。$G/Sc(V)$ が半単純型（ある非可換単純群 N の自己同型群の部分群である場合）であれば、それは表 2 にまとめられている形であり、アフィン型（$\mathcal{S}$ 上正則な基本可換群を正規部分群に持つ）であれば、それは表 3 の群のいずれかの形である。表 2 の 2, 3、5 列には、正規な非可換単純群 N の形、置換表現の次数、$|G/N|$ の可能性の最大値がそれぞれ与えられている。いずれにせよ、stabilizer $G_X/Sc(V)$ の形は限定される。

上の二つの方法で求められた $G_X/Sc(V)$ の構造を比較することにより、$G/Sc(V)$ が半単純型である場合には 定理 3 の場合 (2) が生じることが帰結される。$G/Sc(V)$ がアフィン型であれば、$q = 2$ であって定理 3 の場合 (1) が起こるか、または Huybrechts-Pasini の定理 2 の場合 (3) に相当する結論が得られる。後者の場合には、$G/Sc(V)$ はアフィン型の二重可移群で、q は奇数で、$|\mathcal{S}| = ((q^{d+1}-1)/(q-1))+1$ は 2 のべきである。

後者の場合は、次のように消去される。ここで重要なのは、ambient space V が奇標数 p のベクトル空間であり、G の部分群の通常表現を与えることである。まず $q \equiv 1, d \equiv 2 \pmod 4$, $d \geq 6$ が示される。$G/Sc(V)$ の正則正規部分群を $N/Sc(V)$ とし、T を N の 2-シロー部分群とする。T が非可換である場合には、T のどの特性真部分群も可換であることが示され、T は extraspecial group E と巡回群 R の中心積であることが帰結される。V が与える E の通常表現を考えると、これは忠実である事が示される。従って、V 中の $GF(q)[E]$-既約成分 W は $GF(q)$ 上 2^m 次元であることがわかる。ここで $|E| = 2^{1+2m}$ としている。一方、$|N/Sc(V)| = |T/T \cap Sc(V)| = |E/Z(E)| = 2^{2m}$ であることが示され、これと $N/Sc(V)$ の正則性から $\sqrt{(q^{d+1}-1)/(q-1)+1} = 2^m = \dim_{GF(q)}(W)$ である。一方、$q > 2$ なので、ambient space の次元に対する私の結果 [10] より $\dim_{GF(q)}(V) \leq (d+1)(d+2)/2$ である。従って、

$$\sqrt{q^d + q^{d-1} + \cdots + q + 2} = \dim_{GF(q)}(W) \leq \dim_{GF(q)}(V) \leq (d+1)(d+2)/2$$

という不等式が得られるが、これから矛盾が導かれる。

T が可換なときには、この群は基本可換群になり、G_X のある部分群 H を取ると、$T:H$ は T を核とする Frobenius 群であることが示される。そこで、V が与える Frobenius 群 $T:H$ の通常表現の既約部分加群の次元を $|H|$ を用いて表現できる。H として十分大きな群を取ることが出来るので、上と同様の評価から（円周等分多項式の q での値の評価その他、多少面倒な議論を用いて）、同様に矛盾を得る。詳細は、論文 [13] を参照されたい。

4 小さな ambient space を持つ二重可移な DHO の分類

4.1 特徴付け定理

$GF(q)$ 上定義された d-DHO $\mathcal{S}$ の ambient space $\mathbf{A}(\mathcal{S})$ の次元は $2d+1$ 以上であり、$2d+1$ であるのは、どの X, Y に対しても $\langle X, Y\rangle$ が一定であるときに限る。$q=2$ の場合には、このような構造が得られるための判定条件があるが、$q>2$ の時には、はっきりしない。

$\dim_{GF(q)}(\mathbf{A}(\mathcal{S}))=2d+2$ を満たす二重可移な d-DHO の例は $\mathcal{S}^{d+1}_{\sigma,\tau}$ である（表 1 参照）が、これらの d-DHO を次のように特徴付けすることが出来る。ここで σ と τ は絶対ガロア群 $\mathrm{Gal}(GF(q)/GF(2))$ の生成元であり、$\sigma\tau \neq id_{GF(q)}$ を満たしている。更に $\mathrm{Aut}(\mathcal{S}^{d+1}_{\sigma,\tau})$ は translation のなす正則正規部分群 N を含み、一つのメンバー $X \in \mathcal{S}^{d+1}_{\sigma,\tau}$ の stabilizer は X 上の Singer cycle ($X^{\#}=X-\{0\}$ 上に正則に作用する巡回群) を含んでいることに注意しよう。また、定理 3 により、$GF(q)$ 上定義された二重可移な d-DHO $\mathcal{S}$ に対して、$\mathcal{S}$ が Mathieu DHO でなければ $q=2$ であって、その自己同型群はアフィン型の二重可移群であった。

定理 4 *[14]* $\mathcal{S}$ を $GF(2)$ 上定義された二重可移な *d-DHO* で、その *ambient space* V の次元が $2(d+1)$ であるものとする。$\mathrm{Aut}(\mathcal{S})$ におけるメンバー $X \in \mathcal{S}$ の *stabilizer* が、X の非零ベクトル全体に正則に作用するような巡回群 S を含むと仮定する。$d=5$ の時には、更に交換子 $[V,N]$ の非零ベクトル上の S-軌道の長さはみな等しいと仮定する。ここで N とは、アフィン型二重可移群 $\mathrm{Aut}(\mathcal{S})$ の正則正規部分群を表す。

このとき、絶対ガロア群 $\mathrm{Gal}(GF(q)/GF(2))$ の生成元 σ, τ で $\sigma\tau \neq id_{GF(q)}$ を満たすものが存在して、$\mathcal{S}$ は $\mathcal{S}^{d+1}_{\sigma,\tau}$ と同型である。

この結果の系として、ambient space の次元が $2d+2$ であるような二元体上定義された二重可移な d-DHO のかなり精密な分類を与えることが出来る。特に、$\mathcal{S}^{d+1}_{\sigma,\tau}$ が次のように特徴付けされる [14]。

系 5 $2^{d+1}-1$ と $d+1$ が互いに素とする。二元体上定義された *d-DHO* $\mathcal{S}$ の *ambient space* の次元が $2d+2$ であるとする。このとき、$\mathcal{S}$ が二重可移であることと、$\mathcal{S}$ が適当な $\mathrm{Gal}(GF(q)/GF(2))$ の生成元 σ, τ $(\neq \sigma^{-1})$ に対する $\mathcal{S}^{d+1}_{\sigma,\tau}$ に同型である事は同値である。

Ambient space の次元が $2d+1$ の場合には、定理 4 の類似は得られていない。これは、後述するように、ある合同式を満たす自明な解が存在してしまうという理由による。

4.2 定理 4 の証明のあらまし

定理 4 の証明の大筋を述べよう。以下、$\mathcal{S}$ は定理の仮定を満たす d-DHO とし、$G = \mathrm{Aut}(\mathcal{S})$, $V = \mathbf{A}(\mathcal{S})$, S は $X \in \mathcal{S}$ の stabilizer G_X の部分群で定理の仮定を満たすものとする。また、G は $\mathcal{S}$ 上の置換群と見て、アフィン型の二重可移群であるが、N をその正則正規部分群とする。このとき N は位数 2^{d+1} の基本可換群である。仮定から S は N の自明でない元全体 $N^\times$ に、共役により正則に作用する。

まず、以下の事実が順に示される。

Step 1 $[V,N]$ を $v \in V$, $n \in N$ に対する交換子 $v + v^n$ 全体の生成する V の部分空間とするとき、$V = X \oplus [V,N]$ であり、$1 \neq n \in N$ に対して $\langle X, X^n \rangle \cap [V,N] = [X,n]$ $(:= \{x + x^n \mid x \in X\})$.

Step 2 S は X と $[V,N]$ の双方に既約に作用する。

Step 3 $C_V(N) = \{v \in V \mid v^n = v (\forall n \in N)\} = [V,N]$.

これらから、V は $GF(2)$ 上の $d+1$ 次元のベクトル空間 X と $[V,N]$ の直和であり、巡回群 S は X 上の Singer cycle として作用し、$[V,N]$ 上には Singer 群の部分群を引き起こす。そこで、V と $GF(q) \oplus GF(q)$ の間に、次のような同一視が出来る。

X は $\{(x,0) \mid x \in GF(q)\}$ に対応し、
$[V,N]$ は $\{(0,y) \mid y \in GF(q)\}$ と対応する。

しかも、この同一視の元で S の V への作用は次のように与えられる。ある整数 ε $(0 \leq \varepsilon \leq 2^{d+1}-1)$ があり、任意の $t \in GF(q)^\times$ に対して S の元 $g(t)$ が定まって、$g(t^{-1}) = g(t)^{-1}$ 及び次を満たす。

$$(x,y)^{g(t)} = (tx, t^\varepsilon y). \quad (x,y \in GF(q)) \tag{3}$$

さてこれらの準備の元で、$\mathcal{S}$ が適当な $\sigma, \tau \in \mathrm{Gal}(GF(q)/GF(2))$ に対して $\mathcal{S}^{d+1}_{\sigma,\tau}$ の形に書けることを次のように示すことが出来る。

$1 \neq n \in N$ を固定する。$x \in GF(q)$ に対して $(x,0) + (x,0)^n$ は $[X,n] \leq [V,N]$ の元であるから、上の同一視により $(x,0) + (x,0)^n = (0, f(x))$ を満たす $f(x) \in GF(q)$ が存在する。写像 $GF(q) \ni x \mapsto f(x) \in GF(q)$ は $GF(2)$-linear であるから、$f(X) = a_0 X + a_1 X^2 + \cdots + a_i X^{2^i} + \cdots + a_d X^{2^d}$ という形の多項式 $f(X) \in GF(q)[X]$ により表現される。

すると、任意の $x, y \in GF(q)$ に対して Step3 より $(0,y)^n = (0,y)$ であることなどを使うと

$$\begin{aligned} (x,y)^n &= (x,0)^n + (0,y)^n \\ &= (x,0) + (0,f(x)) + (0,y) = (x, y + f(x)) \end{aligned} \tag{4}$$

である。そこで $(x,y)^{g(t)^{-1}ng(t)}$ を式 (3) と式 (4) を用いて計算すると、$g(t)^{-1}=g(t^{-1})$ であるから

$$\begin{aligned}(x,y)^{g(t)^{-1}ng(t)} &= (t^{-1}x,t^{-\varepsilon}y)^{ng(t)}\\ &= (t^{-1}x,t^{-\varepsilon}y+f(t^{-1}x)^{g(t)}=(x,y+t^{\varepsilon}f(t^{-1}x)) \qquad (5)\end{aligned}$$

を得る。ところで、任意の異なる元 $s,t\in GF(q)^\times$ に対して $g(t)^{-1}ng(t)$ と $g(s)^{-1}ng(s)$ は $N^\times$ の相異なる元であるから、それらの積も $N^\times$ の元である。従って、$u\in GF(q)^\times$ が一意的に存在して、

$$g(t)^{-1}ng(t)\cdot g(s)^{-1}ng(s)=g(u)^{-1}ng(u)$$

を満たす。この式の両辺を $(x,y)\in V$ に作用させて、上の結果 (5) を使うと、「すべての $x\in GF(q)$ に対して $s^{\varepsilon}f(s^{-1}x)+t^{\varepsilon}f(t^{-1}x)=u^{\varepsilon}f(u^{-1}x)$」という結論を得る。これを、多項式 $f(X)$ を用いて書き表せば、
「すべての $i=0,1,\dots,d$ に対して $(s^{\varepsilon-2^i}+t^{\varepsilon-2^i}-u^{\varepsilon-2^i})a_i=0$」である。

従って、任意の $i=0,\dots,d$ に対して、次のどちらかが成立する。

- $a_i=0$.
- 全ての相異なる $s,t\in GF(q)^\times$ に対して、(s,t に依存するが、i に**依存しない**) ある $u\in GF(q)^\times$ が存在して $s^{\varepsilon-2^i}+t^{\varepsilon-2^i}=u^{\varepsilon-2^i}$.

ここで、同一視をうまく取るとき $a_0=1$ 及び $f(1)=a_0+\cdots+a_d=0$ と出来ることが示せる。従って、少なくとも一つの i $(1\le i\le d)$ が存在して $a_i\neq 0$ である。

重要なのは、次が示せることである。

$1\le i\le d$ 及び $a_i\neq 0$ を満たす i は唯一つである。

この部分の証明には、$2^{d+1}-1$ を法としたある合同式を解く必要がある。Ambient space の次元が $2d+1$ と仮定したときも、ほぼ同じ議論でこの合同式まで到達するが、自明な解を消すことが出来なくなり、何も結論が得られなくなる。議論は細かいので論文 [14] を参照されたい。

ともかく $f(X)=X+a_iX^{2^i}$ $(1\le i\le d)$ という形が決まった。$\varepsilon-1$ が $\bmod 2^{d+1}-1$ で逆元を持つことは示せるので、$x^\tau=x^{(\varepsilon-\sigma)(\varepsilon-1)^{-1}}$ により $GF(q)^\times$ 上の写像 τ を定めることが出来る。これを $0^\tau=0$ として $GF(q)$ 上に拡張する。また、$GF(q)$ 上の写像 σ を $x^\sigma=x^{2^i}$ により定める。このとき σ,τ は $\mathrm{Gal}(GF(q)/GF(2))$ の生成元になることが示される。しかも $t\in GF(q)^\times$ に対して $s:=t^{\varepsilon-\sigma}$ とおけば

$$t^{\varepsilon}f(t^{-1}x)=s^\tau x+sx^\sigma$$

となるので、$\mathcal{S}$ の任意のメンバー $X^{g(t)^{-1}ng(t)}$ の次の表示を得る。

$$\begin{aligned}X^{g(t)^{-1}ng(t)} &= \{(x,t^{\varepsilon}f(t^{-1}x)) \mid x\in GF(q)\}\\ &= \{(x,sx^\sigma+s^\tau x) \mid x\in GF(q)\}\end{aligned}$$

これは $\mathcal{S}_{\sigma,\tau}^{d+1}$ のメンバー $X(s)$ の表示に他ならない。従って、望む結論 $\mathcal{S}=\mathcal{S}_{\sigma,\tau}^{d+1}$ が得られた。

5 二次APN関数から作られるDHO

表 1 を見ると、自己同型群 $\mathrm{Aut}(\mathcal{S})$ が $\mathcal{S}$ 上に可移に作用するが、二重可移ではないような d-DHO $\mathcal{S}$ の例としては、Buratti-Del Fra の DHO のみが知られていることに気付く。この場合の自己同型群は、位数 2^{d+1} の正則正規部分群の、$2^d SL_d(2)$ による分裂拡大である。今年の秋に、simply connected という条件にこだわらなければ、このような例は他にも色々あるということに気付いた。これらの d-DHO は二元体上で定義され、その自己同型群は、位数 2^{d+1} の正則正規部分群の、$Z_{2^{d+1}-1} : Z_{d+1}$ の真部分群による分裂拡大という形になっている。このような例は、APN 関数という概念と密接に関係しており、単項式と同値でない APN 関数が 2005 年頃から発見されていることの直接の帰結である。

定義 6 $q = 2^{d+1}$ とする。q 元体 $\mathbf{F}_q$ 上の写像 f が **APN関数** *(almost perfectly nonlinear)* であるとは、すべての 0 でない $a \in \mathbf{F}_q$ に対して次の式が成立することである。

$$\#\{\ f(x+a) - f(x)\ \mid\ x \in \mathbf{F}_q\ \} \ =\ q/2 \tag{6}$$

暗号等の実際上の要請から、有限体上の関数で、線形写像から最も隔たっているものは、非常に重要らしい。APN 関数という概念は、このような応用面からの要請に応えて登場し、盛んに研究されているが、数学的にも面白いと思う。

写像 f が線形写像であれば $f(x+a) - f(x) = f(a)$ であるから、式 (6) の左辺の値は 1 となる。写像 f が "線形写像から最も離れている" とすれば、式 (6) の左辺の値は、出来るだけ大きなものとなるであろう。x と $x+a$ に対する $f(x+a) - f(x)$ は $\mathbf{F}_q$ の標数が 2 だから一致するので、この最も大きな値として可能なのは $q/2$ である。これを実現する写像を almost perfectly nonlinear と呼ぼうというのである。

奇標数の体上の写像 f に対しては、左辺の値の最大値として考えられるのは q であり、これを実現する関数を planar function と呼んだ。planar function の存在と、ある種の射影（アフィン）平面の存在が同等であることが知られている。APN 関数とは、planar 関数の概念の偶標数版であり、これにどの様な有限幾何学的対象が標準的に結びつくのかは、興味深い。

実は、「二次の」 APN 関数に、二元体上の DHO が結びつけられる。ここで、有限体上の写像が二次であるとは、次のように定義される。

定義 7 $q = 2^{d+1}$ とする。q 元体 $\mathbf{F}_q$ 上の写像 f が **二次** *(quadratic)* であるとは、すべての $x, y, z \in \mathbf{F}_q$ に対して次の式が成立することである。

$$f(x+y+z) + f(x+y) + f(y+z) + f(z+x) + f(x) + f(y) + f(z) = 0.$$

特に $f(0) = 0$ である。次の言い換えは、すぐ確かめられる。

命題 8 $q = 2^{d+1}$ とする。$\mathbf{F}_q$ 上の写像 f に対して、次の条件は同値である。

(1) f は二次である。

(2) $b_f(x,y) := f(x+y)+f(x)+f(y)$ により写像 $b_f : \mathbf{F}_q \times \mathbf{F}_q \to \mathbf{F}_q$ を定義するとき、b_f は（$\mathbf{F}_q$ を $GF(2)$ 上の $d+1$ 次元線形空間と見なして）*bilinear map* である。

(3) f は次の形の多項式 $\tilde{f}(X)$ により表示される: $f(x) = \tilde{f}(x)$ $(\forall x \in \mathbf{F}_q)$. ここで a_{ij}, a_i は適当な $\mathbf{F}_q$ の元である。

$$\tilde{f}(X) = \sum_{0 \le i < j \le d} a_{ij} X^{2^i+2^j} + \sum_{0 \le i \le d} a_i X^{2^i}.$$

「二次の」写像は、二次の多項式で表されるわけではないことに注意して欲しい。一般に、有限体 $\mathbf{F}_q$ 上の写像は $\sum_{0 \le k \le q-1} a_k X^k$ $(a_k \in \mathbf{F}_q)$ の形の多項式により表示できるが、命題 8 の (3) における多項式においては、そこに登場する単項式 X^k のべき指数 k は、2 進展開したときに $2^i + 2^j$ ないしは 2^i の形のものに限るのである。

例 $q = 2^{d+1}$ とする。σ が絶対ガロア群 $Gal(\mathbf{F}_q/\mathbf{F}_2)$ の生成元であるとき（すなわち $d+1$ と互いに素な整数 e に対して $x^\sigma = x^{2^e}$ $(x \in \mathbf{F}_q)$ となるとき）、次の形の写像 f は二次の APN 関数である。これは単項式で与えられ、**Gold 関数**と呼ばれている。

$$f(x) = x^{\sigma+1} = x^\sigma x.$$

この写像 f に対する bilinear map b_f は、次のように与えられる。

$$b_f(x,y) = x^\sigma y + x y^\sigma$$

d-DHO $\mathcal{S}^{d+1}_{\sigma,\tau}$ のメンバーは $X(t) = \{(x, x^\sigma t + x t^\tau) \mid x \in GF(q)\}$ という形をしていた。そこで、$\sigma = \tau$ の場合、d-DHO $\mathcal{S}^{d+1}_{\sigma,\sigma}$ のメンバーは、Gold 関数 f を使って $X(t) = \{(x, b_f(x,t)) \mid x \in GF(q)\}$ という形に表示できる。

この観察は、次の命題 9 に一般化出来る。そこでは、$X(t)$ が線形部分空間になるために f が二次であることが必要になる。また、f が APN 関数であることから、次が言える。この性質が、二つのメンバーの交わりが射影点であることを保証する。

「$b_f(x,t) = 0$」 と 「$x = 0$ or $t = 0$ or $x = t$」 が同値である

命題 9 *(S.Y. 2002年頃?)* $q = 2^{d+1}$ とし、f を有限体 $GF(q)$ 上の任意の二次 *APN* 関数とする。$V = GF(q) \oplus GF(q)$ を二元体上の $2(d+1)$ 次元ベクトル空間と見て、$t \in GF(q)$ によりパラメーター付けられた V の部分集合 $X(t)$ を次のように定める。

$$X(t) := \{(x, b_f(x,t)) \mid x \in GF(q)\}.$$

このとき、$\mathcal{S}^{d+1}[f] := \{X(t) \mid t \in GF(q)\}$ は $GF(2)$ 上定義された *d-DHO* である。その *ambient space* は、全ての $0 \neq t \in GF(q)$ に対して $\{b_f(x,t) \mid x \in GF(q)\}$ が $GF(q)$ の一定の超平面になる場合を除いて、V に一致する。

この形の DHO の自己同型は、著しい特徴を持つ。すなわち、正則に作用する部分群がすぐ見出せるのである。$a \in GF(q)$ に対して V 上の線形写像 τ_a を次のように定義する。

$$\tau_a : (x, y) \mapsto (x, y + b_f(x, a)).$$

すると $X(t)^{\tau_a} = X(t + a)$ がすぐ確かめられるので、τ_a は $\mathcal{S}^{d+1}[f]$ の自己同型であり、$a \neq 0$ ならば $\mathcal{S}^{d+1}[f]$ のメンバーを一つも固定しない。$\tau_a\tau_b = \tau_{a+b}$ であるから、$T := \{\tau_a \mid a \in GF(q)\}$ は、$\mathcal{S}^{d+1}[f]$ 上に正則に作用する部分群をなす。

上の Gold 関数 $f(x) = x^{\sigma+1}$ に対しては $\mathcal{S}^{d+1}[f] = \mathcal{S}^{d+1}_{\sigma,\sigma}$ であるから、その自己同型群は $d > 2$ のとき T の $Z_{q-1} : Z_{d+1}$ による分裂拡大に一致し、二重可移になっている。

一般の二次 APN 関数 f に対する $\mathcal{S}^{d+1}[f]$ の自己同型群の構造を決めるということは当然考えるべきであったのだが、実は次の予想が正しいであろうという風評が邪魔をして、上の結果から先を真剣に考えていなかった。

(予想) 二次 APN 関数はすべて Gold 関数に同値である。

ところが、昨年この予想を覆す例が発見され、しかも続々と見つかっているらしいという情報を今秋に手に入れた。そこで、あわてて色々調べだしたところ、次の結果を得た。

命題 10 $q = 2^{d+1}$ 上の二次 *APN* 関数 f から構成される *d-DHO* $\mathcal{S}^{d+1}[f]$ の自己同型群 $\mathrm{Aut}(\mathcal{S}^{d+1}[f])$ において、上の正則部分群 T は正規部分群であり、従って $\mathrm{Aut}(\mathcal{S}^{d+1}[f])$ におけるメンバー $X(0)$ の *stabilizer* を A と記すとき $\mathrm{Aut}(\mathcal{S}^{d+1}[f]) = T : A$ である。*Stabilizer* A は V の部分空間 $Y := \{(0, y) \mid y \in GF(q)\}$ に作用し、その核 K は位数 1 か 3 である。更に $K \neq 1$ で $d \equiv 2 \pmod 4$ ならば $C_A(K)$ は奇数位数である。

これは中途半端な結果であるが、最終的には A が $Z_{q-1} : Z_{d+1}$ の部分群であることが示せる、と考えている。更に、今まで知られている DHO の例との関連を考えると、残念ながら $\mathcal{S}^{d+1}[f]$ は全く新しいというものではない。

命題 11 $q = 2^{d+1}$ 上の二次 *APN* 関数 f から構成される *d-DHO* $\mathcal{S}^{d+1}[f]$ は *Huybrechts* の *DHO* により *cover* される。

以上は一般論であるが、これを最近発見された二次 APN 関数（単項式に同値ではない）について適用して、幾つか結果を得た。Carlet 氏らの発見した無限系列（複数系列ある）[1] に対しては、現在の所一般的な結果を述べることが出来ないので、省略し、一つだけ、具体的な場合を挙げる。

例 $d = 9$ に対する $q = 2^{10}$ 元体上の次の関数 f は二次の APN 関数である [5]。ここで ω は $GF(2^{10})^\times$ の位数 3 の元とする。

$$f(x) = x^3 + \omega x^{36}.$$

この f に対する $GF(2)$ 上定義された 9-DHO $\mathcal{S}^{10}[f]$ の自己同型群は、次の形になる。

$$\mathrm{Aut}(\mathcal{S}^{10}[f]) \cong 2^{10} : (Z_{33} : Z_5).$$

この例では $X(0)$ の stabilizer A は $Z_{33} : Z_5$ に同型であり、$Z_{q-1} : Z_{d+1} = Z_{1023} : Z_{10}$ の真部分群である。また、A の Y への作用の核は位数 3 である。

References

[1] L. Budaghyan, C. Carlet, P. Felke and G. Leander, An infinite class of quadratic APN functions which are not equivalent to power mappings, preprint, 2005.

[2] P. J. Cameron, Finite permutation groups and finite simple groups, Bull. London Math. Soc., 13 (1981), 1–22.

[3] A. Del Fra, On d-dimensional dual hyperovals, Geom. Dedicata, 79 (2000), 157–178.

[4] A. Del Fra and A. Pasini, The universal representation group of Huybrechts's dimensional dual hyperoval, Innovations in Incidence Geometry 3 (2006), 121–148.

[5] Y. Edel, G. Kyureghyan and A. Pott, A new APN function which is not equivalent to a power mapping,

[6] C. Huybrechts and A. Pasini, Flag-transitive extensions of dual affine spaces, Contrib. Algebra Geom. 40 (1999), 503–532.

[7] M. W. Liebeck, The affine permutation groups of rank 3, Proc. London Math. Soc., 54 (1987), 477-516.

[8] H. Taniguchi and S. Yoshiara, On the dimensional dual hyperovals $\mathcal{S}^{d+1}_{\sigma,\phi}$, Innovations in Incidence Geometry, 1 (2005), 197–219.

[9] S. Yoshiara, A family of d-dimensional dual hyperovals in $PG(2d+1,2)$, Europ. J. Combin. 20 (1999), 589–603.

[10] S. Yoshiara, Ambient spaces of dimensional dual arcs, J. Alg. Combin. 19 (2004), 5–23.

[11] S. Yoshiara, 極空間中の双対弧 (Dimensional dual arcs of polar type), 第２１回代数的組合せ論シンポジウム報告集 (June 28–30, 2004, Shinhu Univ., Matsumoto), p.57–68, October, 2004.

[12] S. Yoshiara, Dimensional dual arcs–a survey, pp.247–266, in: Finite Geometires, Groups, and Computation, eds. A. Hulpke, B. Liebler, T. Penttila, and A. Seress, Walter de Gruyter, Berlin-New York, 2006.

[13] S. Yoshiara, Dimensional dual hyperovals with doubly transitive automorphism groups, submitted for publication, November, 2006.

[14] S. Yoshiara, A characterization of a class of dimensional dual hyperovals with doubly transitive automorphism groups and its applications, preprint, March, 2006.

2007年1月9日提出